Attorney Docket No. NETAP020
Client Reference No. 01.240.01

APPLICATION FOR UNITED STATES PATENT

SIGNATURE BASED NETWORK INTRUSION DETECTION SYSTEM AND METHOD

By Inventors:

Handong Wu
3762 Hughes Ave. Apt. 301
Los Angeles, California 90034
Citizen of Sweden

Steve Schwab
2101 Wendy Way
Manhattan Beach, CA 90266
Citizen of the United States

Rob Peckham
1274 Granville Ave., #3
Los Angeles, CA 90025
Citizen of the United States

Assignee: Networks Associates Technology, Inc.
3965 Freedom Circle
Santa Clara, CA 95054

Entity: Large

RITTER, LANG & KAPLAN LLP
12930 Saratoga Ave., Suite D1
Saratoga, CA 95070
(408) 446-8690

SIGNATURE BASED NETWORK INTRUSION DETECTION SYSTEM AND METHOD

BACKGROUND OF THE INVENTION

The present invention relates generally to communication systems, and more particularly, to a signature based network intrusion detection system and method.

The explosion of the Internet allows companies and individuals real time access to vast amounts of information. As Internet access costs have decreased, corporations are increasingly using the Internet for corporate data and communications. The many advantages of the Internet, such as cost and flexibility are heavily impacted by security risks. Security is increasingly becoming a critical issue in enterprise and service-provider networks as usage of public networks for data transport increases and new business applications such as e-commerce sites are deployed. Security measures are required, for example, to prevent hackers from gaining unauthorized access to a corporations information resources or shutting down an e-commerce web site via a distributed denial of service attack. Corporations continue to deploy firewalls to prevent unauthorized users from entering their networks. However, corporations are looking to additional security

technologies to protect their system's vulnerability that firewalls alone cannot address.

One of these additional security measures is an intrusion detection system (IDS). As network attacks have increased in number and severity, intrusion detection systems have become a necessary addition to the security infrastructure of most organizations. Intrusion detection allows organizations to protect their systems from threats that come with increasing network connectivity and reliance on information systems. Intrusion detection systems include software or hardware systems that automate the process of monitoring events occurring in a computer system or network, and analyzing them for signs of security problems. Intruders attempt to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network. These include, for example, unauthorized users, authorized users of the systems who attempt to gain additional privileges for which they are not authorized, and authorized users who misuse the privileges given to them. Intrusion detection technology is therefore, a necessary addition to every large organization's computer network security infrastructure.

Network based intrusion detection systems (NIDSs) provide network surveillance by analyzing packet data streams within the network, searching for unauthorized activity, such as attacks by hackers, and enabling users to respond to security breaches before systems are compromised. Typically, network intrusion

detection systems analyze individual packets flowing through a network and can detect malicious packets that are designed to be overlooked by a firewall's simplistic filtering rules. Network intrusion detection systems may also be configured to look at the payload within a packet to see which particular web server program is being accessed and with what options, and to raise alerts when an attacker tries to exploit a bug in such code. When unauthorized activity is detected, the intrusion detection system can send alarms to a management console or system administrator with details of the activity and may also direct other systems to cut off the unauthorized sessions.

Network intrusion detection systems may be signature based, anomaly based, or a combination of both. The signature based intrusion detection system analyzes information it gathers and compares it to a large database of attack signatures. The system looks for a specific attack that has already been documented. In the anomaly based system, a system administrator defines the baseline, or normal state of the network's traffic load, breakdown, protocol, and typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies. Conventional network intrusion detection devices are challenged with accurately detecting various intrusions hidden in ever increasing high-speed network traffic packets, either via intrusion signature matching or network traffic anomaly discovery approaches.

Conventional signature based network intrusion detection systems treat signatures as passive items. When a packet is inspected, it is matched against a list of signatures. Since a signature database often contains hundreds or thousands of signatures, it is impossible to match the signatures against every packet in real-time in order to detect all potential threats in high-speed network systems.

Furthermore, conventional packet classification techniques are not well suited for handling the diverse nature of intrusion signatures. Signature based intrusion detection systems such as Snort programs are typically configured with a set of rules to detect popular attack patterns. Signature detection systems go one step beyond packet filters in complexity by searching for an arbitrary string that can appear anywhere in the packet payload. Systems such as Snort examine one rule at a time. Each time a rule matches, Snort does a fast string search on the associated pattern using the Boyer-Moore algorithm. While the Boyer-Moore algorithm is very fast for a single string search, a single packet can match several rules with patterns, resulting in many Boyer-Moore searches. Thus, this technique does not scale with increasing rule sizes.

There is, therefore, a need for a system and method for reducing the amount of processing required for packet inspection to provide efficient signature based intrusion detection for high-speed networks.

SUMMARY OF THE INVENTION

A signature based intrusion detection method and system are disclosed. A method for detecting intrusions on a network generally comprises storing signature profiles identifying patterns associated with network intrusions in a signature database and generating classification rules based on the signature profiles. Data packets transmitted on the network and having corresponding classification rules are classified according to generated classification rules. Classified packets are forwarded to a signature engine for comparison with signature profiles.

An intrusion detection system of the present invention generally comprises a signature classifier having a first stage classifier operable to classify packets according to at least one packet field into groups and a second stage classifier operable to classify the packets within each of the groups according to packet type or size. A signature database is provided for storing signature profiles identifying patterns associated with network intrusions. The system further includes a flow table configured to support table lookups of actions associated with classified packets and a signature engine operable to perform a table lookup at the flow table to select an action to be performed on the packet based on its classification. One of the actions is comparing the packets to at least a subset of the signature profiles.

In another aspect of the invention, a computer program product for detecting intrusions on a network generally comprises code that stores signature profiles identifying patterns associated with network intrusions in a signature database, code that generates classification rules based on the signature profiles, code that receives packets transmitted on the network, code that classifies the packets according to at least one packet field into groups, code that classifies the packets within each of the groups according to packet type or size, and code that performs a table lookup to select an action to be performed on the packet based on its classification. One of the actions is comparing the packets to at least a subset of the signature profiles. A computer-readable storage medium is provided for storing the codes.

The above is a brief description of some deficiencies in the prior art and advantages of the present invention. Other features, advantages, and embodiments of the invention will be apparent to those skilled in the art from the following description, drawings, and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram illustrating a signature based intrusion detection system of the present invention.

Fig. 2 is a block diagram illustrating the signature based intrusion detection system of Fig. 1 coupled with a network analysis device.

Fig. 3 is a diagram illustrating an example of network system containing intrusion detection systems of the present invention.

Fig. 4 is an example of a packet flow diagram for the detection system of Fig 2.

Fig. 5 is a block diagram of a signature classifier of the intrusion detection system of Fig. 1.

Fig. 6 is a diagram illustrating a computer system that may be used to execute software of this invention.

Fig. 7 is a flowchart illustrating a signature based intrusion detection process of the present invention.

Corresponding reference characters indicate corresponding parts throughout the several views of the drawings.

DETAILED DESCRIPTION OF THE INVENTION

The following description is presented to enable one of ordinary skill in the art to make and use the invention. Descriptions of specific embodiments and applications are provided only as examples and various modifications will be readily apparent to those skilled in the art. The general principles described herein may be applied to other embodiments and applications without departing from the scope of the invention. Thus, the present invention is not to be limited to the embodiments shown, but is to be accorded the widest scope consistent with the principles and features described herein. For purpose of clarity, details relating to technical material that is known in the technical fields related to the invention have not been described in detail.

Referring now to the drawings, and first to Fig. 1, a signature based intrusion detection system of the present invention is shown and generally indicated at 14. As described in detail below, signature based intrusion detection system 18 uses classification techniques to reduce the number of signatures to be tested for a match, as well as the number of packets that must be examined. The system includes a signature engine 34, classification rules database 40, signature database/parser 42, log file 36 and signature classifier 45. The signature classifier 45 filters out incoming packet streams in accordance with classification rules generated from the

signature database 42. Only packets matched with the classification rules move to the signature engine 34, while no further processing is performed on the rest of packets. The workload of the signature engine 34 is thus reduced. As further described below, the output of the signature classifier 45 may be stored in a flow table and later processed by the signature engine 34. Alternatively, the result may be fed directly to the signature engine.

The signature based intrusion detection system 14 may be used alone or in combination with a data monitoring and analysis device configured to perform fault and network performance management as shown in Fig. 2. The network analysis device is configured to provide network monitoring, protocol decoding, and analysis capabilities. The network analysis device 16 may be, for example, a system such as SNIFFER™, available from Sniffer Technologies, a Network Associates Company. The combination of an intrusion detection device 14 and a network analysis device 16 allows for efficient detection of intrusions in high-speed network traffic since the functionality of system components can be used to perform dual simultaneous functions. The system performs packet capturing, protocol decoding, signature matching, and alert/alarm generation and report or any combination thereof, as described below. Functions such as packet capturing, protocol decoding, network statistics gathering, network traffic diagnosis, and alert/alarm generation and reporting are provided by the network analysis device 16. These applications are leveraged by the intrusion detection system 14 to provide an efficient network

intrusion detection system which may be provided in combination with network analysis and management. Application program interfaces (APIs) may be provided to open applications of the network analysis device 16 (Fig. 1). The APIs are used to parse, generate and load signatures, invoke corresponding signature detection methods from appropriate protocol contexts, access states required for stateful intrusion detection, and access alerts/alarms management facilities.

It is to be understood, however, that the signature based intrusion detection system 14 described below may be used without the network analysis device 16, without departing from the scope of the invention. In this case, certain attributes of the analysis device 16, such as packet decoding, would be incorporated within the intrusion detection device 14.

The present invention operates in the context of a data communication network including multiple network elements. The network may be wireless, frame relay, T1 links, Gigabit Ethernet Local Area Networks (LANs), packet over SONET, Wide Area Networks (WANs), or Asynchronous Transfer Mode (ATM), for example. Fig. 3 illustrates an exemplary network incorporating intrusion detection and analysis systems 18 of the present invention. The network intrusion detection system (NIDS) 18 may be placed at key points throughout the network. The units monitor network traffic, perform local analysis of the traffic, and report attacks to a central management station (e.g., system administrator). The network intrusion

detection systems 18 are preferably placed on the network perimeter including both sides of a firewall 20 (e.g., between router 22 and the Internet), near a web server 26, and on links to internal or partner networks (e.g., between router 28 and internal corporate network 24). For example, NIDS 1 monitors all traffic passing into and out of the internal network. NIDS 1 provides an early warning since it detects reconnaissance port scans that typically indicate the start of hacker activity. From this point, NIDS 1 can document the number and types of attacks originating on the Internet that target the network. NIDS 2 monitors traffic that has passed through the firewall 20. NIDS 3 monitors traffic passing into and out of internal corporate LAN 24. It is to be understood that the network of Fig. 3 is only one example illustrating placement of NIDSs within a network and that the present invention may be used on different types of networks and placed in various locations throughout the network. Furthermore, it is to be understood that the system of the present invention may also be used in networks which are not connected to the Internet and may be used, for example, in intranets or any other type of network.

An initialization routine is used to parse the signatures and detection rules and set up other internal data structures. The signatures are provided to the parser which generates code to be used by signature engine 34 (Fig. 1). The signature engine 34 analyzes the packets to see if there is an intrusion embedded in the packet. Information on detected intrusions is sent to the log file 36, which is available, for example, to a system administrator. The log file 36 may also include an application

that generates alarms for the system administrator. The log file 36 may generate routine reports and other detailed information. A report may contain, for example, system events and intrusions detected over a reporting period. The system may use both active and passive measures when an intrusion is detected. Active measures may involve some automated intervention on part of the system. The passive measures involve reporting intrusion detection system findings to a system administrator or other personnel, who can then take action based on the reports.

Signatures (or patterns) of all known attacks are described in an abstract form and included within the signature database 42. These patterns are used to identify an intrusion. Additional signatures are identified by studying system audit information in order to find matching patterns of known system intrusions. In a similar manner indications of other attacks can be figured out. They are represented in a specified form and coded to the intrusion detection system. A signature analysis or pattern matching algorithm is used upon the packets, wherein the packets are compared to "attack signatures", or signatures of known policy violations or patterns of misuse. Signature engine 34 compares monitored traffic with attack signatures. Attack signatures can comprise, for example, a rules-based hierarchy of traffic signatures of known policy violations. The signature engine 34 compares packets from the network traffic with such attack signatures such that policy violations can be discovered.

Fig. 4 illustrates packet flow through the network intrusion detection and analysis system 18. The system preferably receives raw network packets and uses a network adaptor that listens and analyzes all traffic in real-time as it travels across the network. The packets are received at receiving port (RX) 50 at the MAC (Medium Access Control) layer 52. The packets then pass through IP fragment and CRC (Cyclic Redundancy Checking) 54. Signature classification is first performed at 53 to reduce the workload of the signature engine 34 during signature matching. A statistics filter 56 may also be used to filter out unwanted packets. The filter 56 determines which data to examine more closely and screens out all other network traffic. Filter 56 improves system performance by allowing known nonmalicious traffic to be filtered out. Network statistics are then collected at a statistics collection application 58. A trigger 60 is used to trigger the capture engine 32 to capture packets at 62. The packets are either analyzed in real time or temporarily stored for later analysis. Data may be captured, for example, at a buffer at the full-line rate for a short duration, with subsequent analysis of the buffered data at a slower pace. Protocol decoding 64 is provided to decode a wide range of protocols covering all of the Open System Interconnection (OSI) layers to provide detailed data and analysis. Detailed decoding allows visibility into the network regardless of the speed or topology. The packets may be grouped into different protocol presentations and the packets assembled into high level protocol groups for analysis. Signature matching

66 is performed based on packet classifications to detect network intrusion. Any problems detected are sent to an alert log 68 and appropriate action is taken.

Fig. 5 is a block diagram illustrating details of the signature classifier 45 of the intrusion detection system. The signature classifier 45 includes a first stage classifier 70, second stage classifier 72, flow table 74, and classification rules database 40. The classification rules are generated based on the type of signature entries in the signature database. The classification rules are driven from the signature database so that it will only deal with the flows that will be examined by the active signatures stored in the database. The classification rules may have the following format, for example:

Flow-identity -> Action

Flow-identity:

<prototype type>

<source ip address>

<destination ip address>

<source ip address, destination ip address>

<source ip address, range of dest ip addresses>

<range of source ip addresses, destination ip address>

<range of source ip addresses, range of destination ip addresses>

<source port number>

<destination port number>

Action:

[pass to signature engine]

[drop]

The following is an example for a SNORT type signature:

alter tcp any-source-ip-address any-source-port-> 192.5.49.200 80

The resulting classification rule is:

<destination-ip address=192.5.49.200, destination–port-number=80, tcp>[pass to signature engine]

Similar signatures may be combined to generate a single classification rule.

The signature classifier 45 groups packets into separate flows (e.g., TCP, UDP, or HTTP). Each identified flow may be handled differently by the signature engine to speed up the process. The signature classifier may be constructed with single or multiple stages. The signature classifier 45 shown in Fig. 5 performs a multi-stage classification process. The first stage of classification is based on a selected set of packet fields, such as destination address, protocol type, and destination port number. The second classification stage may be based on packet type or size (e.g., TCP flags or packet length). The table 74 supports efficient table

lookups of appropriate actions associated with incoming packets. When a packet is captured and classified, the appropriate entry of the flow table 74 is retrieved in order to perform the associated action. The action options may include, for example, match the packet against a given subset of signatures, drop the packet, generate an alert, or drop the packet and update one or more fields of the flow table 74. As a default, all unclassified packets are dropped. It is to be understood that the flow table 74 may include different action options without departing from the scope of the invention. The flow table 74 may be implemented as one or more hash tables or other suitable data structures.

The signature engine 34 is responsible for identifying any intrusion embedded in the incoming packets selected by the signature classifier 45. The signature engine 34 preferably uses a priority scheme to ensure that a small set of signatures are checked when the system is overloaded with a large number of incoming packets. This allows the system administrator or security officer to identify and catch the most serious attacks.

Fig. 6 is a system block diagram of a computer system, generally indicated at 78, that may be used within the network to execute software of an embodiment of the invention. The computer system may include subsystems such as a central processor 80, system memory 82, removable storage 86 (e.g., CD-ROM drive), and a hard drive 84 which can be utilized to store and retrieve software programs incorporating

computer code that implements aspects of the invention, data for use with the invention, and the like. The computer readable storage may also include tape, flash memory, or system memory. Additionally, a data signal embodied in a carrier wave (e.g., in a network including the Internet) may be the computer readable storage medium. The computer system 78 may further include a display screen, keyboard, and mouse which may include one or more buttons for interacting with a GUI (Graphical User Interface). Other computer systems suitable for use with the invention may include additional or fewer subsystems. For example, the computer system 78 may include more than one processor 80 (i.e., a multi-processor system) or a cache memory.

The system bus architecture of the computer system 78 is represented by arrows 88 in Fig. 6. However, these arrows are only illustrative of one possible interconnection scheme serving to link the subsystems. For example, a local bus may be utilized to connect the central processor 80 to the system memory 82. The components shown and described herein are those typically found in most general and special purpose computers and are intended to be representative of this broad category of data processors. The computer system 78 shown in Fig. 6 is only one example of a computer system suitable for use with the invention. Other computer architectures having different configurations of subsystems may also be utilized.

Communication between computers within the network is made possible with the use of communication protocols, which govern how computers exchange information over a network. The computer may include an input/output circuit used to communicate information in appropriately structured form to and from the parts of computer and associated equipment. Connected to the input/output circuit are inside and outside high speed Local Area Network interfaces 90, for example. The inside interface may be connected to a private network, while the outside interface may be connected to an external network such as the Internet. Preferably, each of these interfaces includes a plurality of ports appropriate for communication with the appropriate media, and associated logic, and in some instances memory.

Fig. 7 is a flowchart illustrating a process of the present invention for performing signature based intrusion detection. The packets are first received at the intrusion detection system at step 100 and filtered at step 102. Remaining packets are captured by the capture engine at step 104. The protocols are decoded at step 106. The classification rules are generated and loaded at step 108. The packets are then classified by the first and second stage classifiers 70, 72 to prepare them for signature matching (step 110). The signatures are partitioned into disjoint groups and each packet is analyzed (step 112). For example, all TCP flows may be separated from UDP flows, and HTTP flows may be separated from SMTP flows. After signature matching is performed, appropriate action is selected for each packet (step 114). Action may include, for example, match packet with subset of signatures

(step 116), drop packet (step 118), generate alarm (120), or drop packet and update field of flow table (step 122).

As can be observed from the foregoing, the system and method of the present invention provide numerous advantages. The classification system of the present invention reduces the amount of work required for packet inspection. The system and method of the present invention reduces downtime caused by undetected attacks, resulting in greater availability of systems to conduct internal operations and complete transactions over the Internet or other communication network.

Although the present invention has been described in accordance with the embodiments shown, one of ordinary skill in the art will readily recognize that there could be variations made to the embodiments without departing from the scope of the present invention. Accordingly, it is intended that all matter contained in the above description and shown in the accompanying drawings shall be interpreted as illustrative and not in a limiting sense.